RIPHAH INTERNATIONAL UNIVERSITY

FACULTY OF COMPUTING, FEMALE

GULBERG GREEN CAMPUS

Bachelor of Software Engineering, Semester 7

Mid Term Examinations, Fall 2023

Course: *Information Security*

Time Allowed: **2 hrs**

Total marks: 70

SAP ID:

Name:

Instructions: Attempt all questions.

Q. No. 01. Encircle the correct option. **(30 Marks)**

1. Which of the following *best* expresses the primary goal when controlling access to assets?

a. Preserve confidentiality, integrity, and availability of systems and data.
b. Ensure that only valid objects can authenticate on a system.
c. Prevent unauthorized access to subjects.
d. Ensure that all subjects are authenticated.

2. Which of the following is true related to a subject?

A. A subject is always a user account.
B. The subject is always the entity that provides or hosts information or data.
C. The subject is always the entity that receives information about or data from an object.
D. A single entity can never change roles between subject and object.

3. Based on advice from the National Institute of Standards and Technology (NIST), when should regular users be required to change their passwords?

a. Every 30 days
b. Every 60 days
c. Every 90 days
d. Only if the current password is compromised

4. Your organization issues devices to employees. These devices generate onetime passwords every 60 seconds. A server hosted within the organization knows what this password is at any given time. What type of device is this?

a. Synchronous token
b. Asynchronous token
c. Smartcard
d. Common access card

5. Fred, an administrator, has been working within an organization for over 10 years. He previously maintained database servers while working in a different division. He now works in the programming department but still retains privileges on the database servers. He recently modified a setting on a database server so that a script he wrote will run. Unfortunately, his change disabled the server for several hours before database administrators discovered the change and reversed it. Which of the following could have prevented this outage?

a. A policy requiring strong authentication
b. Multifactor authentication
c. Logging
d. Account access review

6. Tonya is performing a risk assessment of a third-party software package for use within her organization. She plans to purchase a product from a vendor that is very popular in her industry. What term best describes this software?

a) It Open source
b) Custom-developed
c) ERP
d) COTS

7. James recently discovered an attack taking place against his organization that prevented employee from accessing critical records. What element of CIA triad was violated?

a) Identification
b) Availability
c) Layering
d) Encryption

8. How is the value of a safeguard to a company calculated?

a) ALE before safeguard – ALE after implementing the safeguard – annual cost of safeguard
b) ALE before safeguard * ARO of safeguard
c) ALE after implementing safeguard + annual cost of safeguard – controls gap
d) Total risk – controls gap

9. When a safeguard or a countermeasure is not present or is not sufficient, what remains?

a) Vulnerability
b) Exposure
c) Risk
d) Penetration

10. Which of the following represents accidental or intentional exploitations of vulnerabilities?

a) Threat events
b) Risks

c) Threat agents
d) Breaches

11. Which of the following would generally not be considered an asset in a risk analysis?
    a) A development process
    b) An IT infrastructure
    c) A proprietary system resource
    d) Users' personal files

12. If an organization contracts with outside entities to provide key business functions or services, such asaccount or technical support, what is the process called that is used to ensure that these entities supportsufficient security?
    a) Asset identification
    b) Third-party governance
    c) Exit interview.
    d) Qualitative analysis

13. When seeking to hire new employees, what is the first step?
    a) Create a job description.
    b) Set position classification.
    c) Screen candidates
    d) Request résumés

14. What ensures that the subject of an activity or event cannot deny that the event occurred?
    a) CIA Triad
    b) Abstraction
    c) Nonrepudiation
    d) Hash totals

15. Which of the following is not considered a violation of confidentiality?

    a) Stealing passwords
    b) Eavesdropping
    c) Hardware destruction
    d) Social engineering

RIPHAH INTERNATIONAL UNIVERSITY

FACULTY OF COMPUTING, FEMALE

GULBERG GREEN CAMPUS

Bachelor of Software Engineering, Semester 7

End Term Examinations, Fall 2023

Course: *Information Security*

Subjective Part

Time Allowed: 1.5 hrs

Total marks: 40

SAP ID:

Name:

Instructions: Attempt all questions.

Note: Attempt all questions.

Q.No.1: Describe the differences between identification, authentication, authorization, and accountability.

Q. No.2 Describe the three primary authentication factor types? What are the advantages and disadvantages of these factor types. What is their application?

Q. No. 03. What is IS governance? What are the responsibilities of IS governance? (5+5)

Q. No. 04. What are the main types of social engineering principles, explain any 3? (10)

Q. No. 05. What is Risk management? Differentiate between risk assessment and risk repose? (5+5)

Good Luck!